Практическая работа

Построение модели вероятного нарушителя

В случае обеспечения безопасности персональных данных без использования криптосредств при формировании модели угроз используются методические документы ФСТЭК России.

В случае определения оператором необходимости обеспечения безопасности персональных данных с использованием криптосредств при формировании модели угроз используются методические документы ФСТЭК России и «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные приказом руководства 8 Центра ФСБ России от 21.02.2008 г. № 149/54-144.

При этом из двух содержащихся в документах ФСТЭК России и Методических рекомендациях однотипных угроз выбирается более опасная.

Различают модель угроз верхнего уровня и детализированную модель угроз.

Модель угроз верхнего уровня предназначена для определения характеристик безопасности защищаемых персональных данных и других объектов защиты. Эта модель также определяет исходные данные для детализированной модели угроз.

Детализированная модель угроз предназначена для определения требуемого уровня криптографической защиты.

Модель нарушителя тесно связана с моделью угроз и, по сути, является ее частью. Смысловые отношения между ними следующие. В модели угроз содержится максимально полное описание угроз безопасности объекта. Модель нарушителя содержит описание предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

С учетом методических рекомендаций ФСБ России **модель нарушителя** должна иметь следующую структуру:

– описание нарушителей (субъектов атак);

– предположения об имеющейся у нарушителя информации об объектах атак;

– предположения об имеющихся у нарушителя средствах атак;

– описание каналов атак.

1. Описание нарушителей (субъектов атак).

Различают шесть основных типов нарушителей: H1, H2, ... , H6.

Предполагается, что нарушители типа H5 и H6 могут ставить работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств.

Возможности нарушителя типа Hi+1 включают в себя возможности нарушителя типа Hi ($1 \leq i \leq 5$).

Если внешний нарушитель обладает возможностями по созданию способов подготовки атак, аналогичными соответствующим возможностям нарушителя типа Hi (за исключением возможностей, предоставляемых пребыванием в момент атаки в контролируемой зоне), то этот нарушитель также будет обозначаться как нарушитель типа Hi ($2 \leq i \leq 6$).

Данный раздел модели нарушителя имеет следующее типовое содержание.

Сначала все физические лица, имеющие доступ к техническим и программным средствам информационной системы, разделяются на следующие категории:

– **категория I** – лица, не имеющие права доступа в контролируемую зону информационной системы;

– **категория II** – лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы.

Далее все потенциальные нарушители подразделяются на:

– внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационной системы;

– внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационной системы.

Констатируется, что:

– внешними нарушителями могут быть как лица категория I, так и лица категории II;

– внутренними нарушителями могут быть только лица категории II.

Дается описание привилегированных пользователей информационной системы (членов группы администраторов), которые назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств криптосредства, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.

Далее следует обоснование исключения тех или иных типов лиц категории II из числа потенциальных нарушителей. Как правило, привилегированные пользователи информационной системы исключаются из числа потенциальных нарушителей.

И, наконец, рассматривается вопрос о возможном сговоре нарушителей.

2. Предположения об имеющейся у нарушителя информации об объектах атак

Данный раздел модели нарушителя должен содержать:

– предположение о том, что потенциальные нарушители обладают всей информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

– обоснованные ограничения на степень информированности нарушителя (перечень сведений, в отношении которых предполагается, что

они нарушителю недоступны). Обоснованные ограничения на степень информированности нарушителя могут существенно снизить требования к криптосредству.

При определении ограничений на степень информированности нарушителя, в частности, должны быть рассмотрены следующие сведения:

– содержание технической документации на технические и программные компоненты;

– долговременные ключи криптосредства;

– все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами (фазовые пуски, синхропосылки, незашифрованные адреса, команды управления и т.п.);

– сведения о линиях связи, по которым передается защищаемая информация;

– все сети связи, работающие на едином ключе;

– все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, нарушения правил эксплуатации криптосредства;

– все проявляющиеся в каналах связи, не защищенных от НСД к информации организационно-техническими мерами, неисправности и сбои технических средств криптосредства;

– сведения, получаемые в результате анализа любых сигналов от технических средств криптосредства, которые может перехватить нарушитель.

Только нарушителям типа Н3 - Н6 могут быть известны все сети связи, работающие на едином ключе.

Только нарушители типа Н5 - Н6 располагают наряду с доступными в свободной продаже документацией на криптосредство исходными текстами прикладного программного обеспечения.

Только нарушители типа Н6 располагают всей документацией на криптосредство.

3. Предположения об имеющихся у нарушителя средствах атак

Данный раздел модели нарушителя должен содержать:

– предположение о том, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну;

– обоснованные ограничения на имеющиеся у нарушителя средства атак.

При определении ограничений на имеющиеся у нарушителя средства атак, в частности, должны быть рассмотрены:

– аппаратные компоненты криптосредства;

– доступные в свободной продаже технические средства и программное обеспечение;

– специально разработанные технические средства и программное обеспечение;

– штатные средства.

Нарушители типа Н1 и Н2 располагают только доступными в свободной продаже аппаратными компонентами криптосредства.

Дополнительные возможности нарушителей типа Н3-Н5 по получению аппаратных компонент криптосредства зависят от реализованных в информационной системе организационных мер.

Нарушители типа Н6 располагают любыми аппаратными компонентами криптосредства.

Нарушители типа Н1 могут использовать штатные средства только в том случае, если они расположены за пределами контролируемой зоны.

Возможности нарушителей типа Н2-Н6 по использованию штатных средств зависят от реализованных в информационной системе организационных мер.

Нарушители типа H4-H6 могут проводить лабораторные исследования криптосредств, используемых за пределами контролируемой зоны информационной системы.

4. Описание каналов атак

С практической точки зрения этот раздел является одним из важнейших в модели нарушителя. Его содержание по существу определяется качеством формирования модели угроз верхнего уровня.

Основными каналами атак являются:

– каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами;

– штатные средства.

Возможными каналами атак, в частности, могут быть:

– каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический);

– машинные носители информации;

– носители информации, выведенные из употребления;

– технические каналы утечки;

– канал утечки за счет электронных устройств негласного получения информации;

– информационные и управляющие интерфейсы СВТ.

Определение типа нарушителя

Нарушитель относится к типу Hi, если среди предположений о его возможностях есть предположение, относящееся к нарушителям типа Hi и нет предположений, относящихся только к нарушителям типа Hj (j > i).

Нарушитель относится к типу H6 в информационных системах, в которых обрабатываются наиболее важные персональные данные, нарушение характеристик безопасности которых может привести к особо тяжелым последствиям.

Рекомендуется при отнесении оператором нарушителя к типу H6 согласовывать модель нарушителя с ФСБ России.

Задание

На основе исходных данных, предоставленных преподавателем, и описанной методики построить модель потенциального нарушителя и описать её в отчете о практической работе.

Варианты заданий (по номеру в журнале)

1. Турфирма.
2. Частная школа.
3. Круизная компания.
4. Пожарная часть.
5. Университет дополнительного образования.
6. Адвокатская контора.
7. Страховая компания
8. Фирма по сборке компьютеров
9. Аптечный склад
10. ТЭЦ
11. Агентство недвижимости
12. Курьерская служба
13. Логистическая компания
14. Система лояльности в магазине
15. Салон красоты
16. Кредитная организация
17. Интернет-кинотеатр
18. Интернет-магазин
19. Визовый центр
20. Сотовый оператор
21. Сеть отелей
22. Мебельный склад.
23. Офис сотовой связи.
24. Завод по производству боевых припасов.
25. Фармацевтическая компания.
26. Ветеринарная клиника.
27. Частный стоматологический кабинет.
28. Авиакомпания.
29. Офис проката автомобилей.
30. Станция скорой помощи.